## ABSTRACT

Systems and methods for executing electronic transactions on an anonymous basis using blind auditable membership proofs. By making use of a new cryptographic primitive, electronic transactions such as payment, voting, investment, redemption of tax coupon, and international currency transfer may be made both anonymous and auditable. In an electronic payment system according to the present invention, a user submits information identifying a coin to a bank which in turn validates the coin and adds it to a public list of valid coins. To make a payment using the coin, the user presents an efficient auditable membership proof to a merchant in the form of a zero knowledge argument which proves that the user knows the authenticating information for an unspecified coin in the public list of valid coins. The merchant verifies the zero knowledge argument, accepts the coin as payment, and presents certain authenticating information to the bank. After verifying the merchant's identity and the validity of the coin referenced in the authenticating information, the bank credits the merchant's account and removes the coin from the public list of valid coins. Thereby the user makes payment with complete anonymity while authorities are given the necessary opportunity to monitor and audit the transactions to help deter and prevent bank robbery, blackmail, money laundering and other illegality.